U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
THE DEPUTY SECRETARY
WASHINGTON, DC 20410-0050

January 13, 2006

MEMORANDUM FOR: Principal Staff

FROM: Roy A. Bernardi

SUBJECT: INFORMATION -- HUD Contingency Planning Policy

In December 2003, the HUD Office of the Inspector General (OIG) released a Final Audit Report on Fiscal Year 2003 Review of Information Systems Controls in Support of the Financial Statements Audit (2004-DP-0001) and found that the Department had not followed the National Institute of Standards and Technology (NIST) guidelines for the development and testing of contingency-related plans. OIG found that there was inadequate assurance that HUD can recover operational capability in a timely and orderly manner in the event of a disaster or other unexpected interruptions.

As recommended by OIG, the attached HUD Contingency Planning Policy has been developed from guidance issued in the NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*. While the NIST publication concentrates on Information Technology (IT) Systems, it recommends a coordinated agency approach to contingency planning that addresses all related agency activities, including IT security, physical security, human resources, IT operations, and emergency preparedness functions.

The Office of Security and Emergency Planning, in coordination with the Office of the Chief Information Officer, will provide further guidance on this in the near future.

Attachment

HUD Contingency Planning Policy

1. PURPOSE

This document defines HUD's overall contingency planning policy and objectives, establishes the organizational framework and responsibilities for contingency planning, and adopts standard terminology for use in developing contingency plans.

2. BACKGROUND

In December 2003, the HUD Office of the Inspector General (OIG) released a Final Audit Report on Fiscal Year 2003 Review of Information Systems Controls in Support of the Financial Statements Audit (2004-DP-0001). The OIG report concluded that the Department had not followed the National Institute of Standards and Technology (NIST) guidelines for the development and testing of contingency-related plans. The OIG report also found that there was inadequate assurance that HUD can recover operational capability in a timely and orderly manner in the event of a disaster or other unexpected interruptions.

The OIG final audit report recommended that the Assistant Secretary for Administration and the Chief Information Officer ensure that the NIST guidelines and other federal requirements for contingency planning are implemented.

3. AUTHORITY

This policy has been developed from guidance issued in the NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*. While the NIST publication concentrates on information technology (IT) systems, it recommends a coordinated agency approach to contingency planning that addresses all related agency activities, including IT security, physical security, human resources, IT operations, and emergency preparedness functions.

4. SCOPE

HUD Handbook 2400.25, Rev. 1, *Information Technology Security Policy*, addresses the contingency planning policy for IT systems (*Section 3.6, Information Technology Contingency Planning*). This document establishes the overall policy for development and management of HUD contingency plans and procedures to ensure that all business processes are addressed, in addition to the IT systems. This policy applies to all HUD offices.

5. POLICY

Contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of systems, operations, and data after a disruption. This document establishes the policy that HUD offices will utilize to ensure that contingency plans are developed in coordination with other agency components.

6. DEFINITIONS

All HUD offices will utilize the following contingency planning definitions, as outlined in NIST 800-34, when developing their contingency plans.

A. **Business Continuity Plan (BCP)**. The BCP focuses on sustaining an organization's business functions during and after a disruption. An example of a business function may be an organization's payroll process or consumer information process. A BCP may be written for a specific business process or may address all key business processes. IT systems are considered in the BCP in terms of their support to the business processes. A disaster recovery plan, business resumption plan, and occupant emergency plan may be appended to the BCP. Responsibilities and priorities set in the BCP should be coordinated with those in the Continuity of Operations Plan to eliminate possible conflicts.

B. **Business Recovery (or Resumption) Plan (BRP)**. The BRP addresses the restoration of business processes after an emergency but, unlike the BCP, it lacks procedures to ensure continuity of critical processes throughout an emergency or disruption. Development of the BRP should be coordinated with the disaster recovery plan and BCP. The BRP may be appended to the BCP.

C. **Continuity of Operations (COOP) Plan**. The COOP Plan focuses on restoring an organization's essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. Implementation of a viable COOP capability is mandated by Presidential Decision Directive (PDD) 67, *Enduring Constitutional Government and Continuity of Government Operations*. FEMA, which is the Federal Government's executive agent for COOP, provides COOP guidance in Federal Preparedness Circular (FPC) 65, *Federal Executive Branch Continuity of Operations*. Standard elements of a COOP Plan include delegations of authority, orders of succession, and vital records and databases. The COOP Plan emphasizes the recovery of an organization's operational capability at an alternate site.

D. **IT Contingency Plan**. OMB Circular A-130, Appendix III, requires the development and maintenance of continuity-of-support plans for general support systems and contingency plans for major applications. Because an IT contingency plan should be developed for each major application and general support system, multiple contingency plans may be maintained within the organization's BCP.

E. **Crisis Communications Plan**. Organizations should prepare their internal and external communications procedures prior to a disaster. A crisis communications plan is often developed by the organization responsible for public outreach. The crisis communication plan procedures should be coordinated with all other plans to ensure that only approved statements are released to the public. Those procedures should be included as an appendix to the BCP. Also, the communications plan typically designates specific individuals as the only authority for answering questions from the public regarding disaster response. The plan may also include procedures for disseminating status reports to personnel and to the public, including templates for press releases.

F. **Cyber Incident Response Plan**. The Cyber Incident Response Plan establishes procedures to address cyber attacks against an organization's IT system(s). These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware, software, or data. This plan may be included among the appendices of the BCP.

G. **Disaster Recovery Plan (DRP)**. As suggested by its name, the DRP applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. Frequently, DRP refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after any emergency. The DRP scope may overlap with an IT contingency plan; however, the DRP is narrower in scope and does not address minor disruptions that do not require relocation. Dependent on the organization's needs, several DRPs may be appended to the BCP.

H. **Occupant Emergency Plan (OEP).** The OEP provides the response procedures for occupants of a facility in the event of a situation posing a potential threat to the health and safety of personnel, the environment, or property. Such events would include a fire, hurricane, criminal attack, or a medical emergency. OEPs are developed at the facility level and are specific to the geographic location and structural design of the building. General Service Administration (GSA)-owned facilities maintain plans based on the GSA OEP template. The facility OEP may be appended to the BCP, but is executed separately.

Table 1 provides a summary of the types of plans discussed above.

Table 1
Types of Contingency-Related Plans

Plan	Purpose	Scope
Business Continuity Plan (BCP)	Provides procedures for sustaining essential business operations while recovering from a significant disruption	Addresses business processes; IT addressed based only on its support for business process
Business Recovery (or Resumption) Plan (BRP)	Provides procedures for recovering business operations immediately following a disaster	Addresses business processes; not IT-focused; IT addressed based only on its support for business process
Continuity of Operations Plan (COOP)	Provides procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site for up to 30 days	Addresses the subset of an organization's missions that are deemed most critical; usually written at headquarters level; not IT-focused
IT Contingency Plan	Provides procedures and capabilities for recovering a major application or general support system	Addresses IT system disruptions; not business process focused
Crisis Communications Plan	Provides procedures for disseminating status reports to personnel and the public	Addresses communications with personnel and the public; not IT-focused
Cyber Incident Response Plan	Provides strategies to detect, respond to, and limit consequences of malicious cyber attack	Focuses on information security responses to incidents affecting systems and/or networks
Disaster Recovery Plan (DRP)	Provides detailed procedures to facilitate recovery of capabilities at an alternate site	Often IT-focused; limited to major disruptions with long-term effects
Occupant Emergency Plan (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat	Focuses on personnel and property particular to the specific facility; not business process or IT system functionality-based

7. PROCEDURES

The following contingency process, as outlined in NIST 800-34, should be considered in developing and maintaining a viable contingency planning program.

A. **Develop the contingency planning policy statement**. A formal department or agency policy provides the authority and guidance necessary to develop an effective contingency plan.
B. **Conduct the business impact analysis (BIA)**. The BIA helps to identify and prioritize critical systems and components.
C. **Identify preventive controls**. Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.
D. **Develop recovery strategies**. Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
E. **Develop a contingency plan**. The contingency plan should contain detailed guidance and procedures for restoring a damaged system.
F. **Plan testing, training, and exercises**. Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness.
G. **Plan maintenance**. The plan should be a living document that is updated regularly to remain current with system enhancements.

8. RESPONSIBILITIES

The following responsibilities have been designated to ensure the contingency plans defined above are developed, managed, and maintained.

The Director of the Office of Security and Emergency Planning (OSEP), in the Office of Administration, is the HUD Contingency Planning Coordinator, and will oversee and monitor contingency planning progress in coordination with the Office of the Chief Information Officer (OCIO) and other Program Offices to ensure the appropriate plans and procedures are developed and maintained. This will include establishing completion schedules and tasking each Program Office with activities addressing their respective program areas.

The Chief Information Officer is the IT Contingency Planning Coordinator, and is responsible for coordinating all contingency plans addressing IT systems. This includes system-level IT Contingency Plans, the Cyber Incident Response Plan, the Disaster Recovery Plan, and assistance with those plans requiring IT support for business processes.

Each Program Office Head will designate a Contingency Planning Point of Contact (POC) who will be responsible for providing the required plans and procedures needed to sustain and/or recover the Program Office's business processes following a disaster or significant disruption. The Director of OSEP, as the HUD Contingency Planning Coordinator, will provide each Program Office Contingency Planning POC with appropriate guidance to ensure a consistent and standard approach.

cc: Principal Staff

Alphonso Jackson, Secretary, S
Camille T. Pierce, Chief of Staff, S
Scott A. Keller, Deputy Chief of Staff, S
James V. Parenti, Senior Advisor to the Deputy Secretary, SD
David Hazelton, Assistant to the Secretary and White House Liaison, S
Marcella E. Belt, Chief Executive Officer, S
Keith E. Gottfried, General Counsel, C
Brian D. Montgomery, Assistant Secretary for Housing – Federal Housing Commissioner, H
Pamela H. Patenaude, Assistant Secretary for Community Planning and Development, D
Orlando J. Cabrera, Assistant Secretary for Public and Indian Housing, P
Darlene F. Williams, Assistant Secretary for Policy Development and Research, R
Kim Kendrick, Assistant Secretary for Fair Housing and Equal Opportunity, E
Keith A. Nelson, Assistant Secretary for Administration, A
Cathy M. MacFarlane, Assistant Secretary for Public Affairs, W
Michael J. Frenz, Executive Vice President, Government National Mortgage Association, T
James M. Martin, Acting Deputy Chief Financial Officer, FM
Steven B. Nesmith, Assistant Secretary for Congressional and Intergovernmental Relations, J
Kenneth M. Donohue, Sr., Inspector General, G
A. Jo Baylor, Assistant Deputy Secretary for Field Policy and Management, M
Inez Banks-Dubose, Director, Office of Departmental Operations and Coordination, I
Robert J. Bogart, Director, Center for Faith-Based and Community Initiatives, K
Michael F. Hill, Acting Director, Office of Healthy Homes and Lead Hazard Control, L
Cynthia A. O'Connor, Executive Secretary, AJF